Method for authenticating a smart card within a messaging network

This invention relates to a method for authenticating a smart card in a messaging network, preferably a GSM network, according to the preamble of claim 1.

In GSM systems it is known that for using the smart card (subscriber identity module, SIM) the user must usually first identify himself as an authorized user by means of a personal identification number (PIN). In order to avoid abuse at this point, it is known to provide an error counter for the PIN entry to prevent further use of the card after a permissible number of failed attempts is exceeded.

A further system-relevant security measure is to authenticate the card vis-à-vis the mobile network. A secret key inaccessible from outside and an algorithm likewise inaccessible from outside are stored in the card. For authentication a random number is generated by the network or a network component and transferred to the card. The card then calculates from the random number and secret key by means of the algorithm present in the card a response which it transfers to the network. This response is analyzed in the network and, if the result is positive, access to the network functions is allowed. The corresponding procedure is described in the relevant GSM specifications.

A network protected as stated above involves the danger that attacks on the algorithm used for authentication permit the network to be simulated in a computer for example by e.g. selected "random numbers" being transmitted to the SIM card according to the standardized protocol and the secret key of the smart card being determined therefrom, after several authentication attempts. If the algorithm of the card is additionally known, essential functional elements of the card can be simulated or duplicated after determination of the secret key.

~~It is therefore the problem of the invention to state a reliable method for~~ authenticating a smart card in a messaging system wherein there is no acknowledgment of the authentication result to the subscribing smart card, as customary in the ~~GSM network for example.~~

~~This problem is solved according to the invention starting out from the features of the preamble of claim 1 by the characterizing features of claim 1.~~

Advantageous embodiments of the invention are stated in the dependent claims.

The invention provides for forming the authentication message by forming at least two parts from both the secret key and the random number transferred by the network, one of the parts of the transferred random number and one or more parts of the secret key being encrypted by means of a one- or multistep, preferably symmetrical calculation algorithm. To output an authentication message, a selectable part of the result calculated according to the authentication algorithm is transferred to the network.

An advantageous embodiment of the invention provides for generating the channel coding key in the same way. There too it is provided that, if key and random number are split into two parts for example, either the first or the second part of the transferred random number is linked with the first and/or second part of the secret key with a one- or multistep algorithm in order to obtain a channel coding key. One preferably uses different parts of the random number obtained from the network for forming the authentication message and the channel coding key in each case.

A further advantageous embodiment of the invention provides that the secret key stored in the card and the random number sent by the network to the card are split into equally long parts. This permits the same calculation algorithm to be used in both cases. The random number or secret key can be split by simply making a split "in the middle" or by creating overlapping partial areas. One can also effect a split by which the sum of the individual parts is smaller than the bit length of the random number or secret key. According to a further variant, a given number of bits of the random number or secret key can be combined into a key or random number part according to a predetermined pattern or pseudorandomly.

As a further advantageous embodiment of the invention, one can use DES algorithms as calculation algorithms for authentication and for channel coding.

Another advantageous variant of the invention provides for using the preferably one-step IDEA algorithm for calculating the authentication parameters and channel coding keys.

Alternatively, one can calculate the authentication parameters and channel coding keys using compression algorithms, preferably cryptographic compression algorithms whose output values have a smaller length than the input parameters.

To increase security it is advantageous to use an at least two-step calculation algorithm, whereby a triple DES algorithm proves especially safe. With this algorithm one first encrypts with a first part of the key and a part of the random number, then performs decryption of the result with the second part of the key, and finally executes a further calculation with the first part of the key again. For the last encryption with the first part of the key one can advantageously use a new, third key, in particular if the key is split into three key parts.

A further advantageous embodiment of the invention results if the selection of the first or second part of the random number is effected alternatingly for authentication and calculation of the channel coding, this alternation being executed randomly or pseudorandomly and the selection being effected in the same way in the card and the network.

The invention will be described more closely in the following with reference to Figures 1 to 3.

Fig. 1 shows the sequence of cryptographic functions of the SIM in the GSM network.

Fig. 2 shows a block diagram of triple DES encryption.

Fig. 3 shows examples of the split of the secret key and random number.

The sequence shown in Fig. 1 assumes that the customary, preceding process of PIN verification has been completed. Subsequently, the mobile unit in which card *SIM* is located sends to the network a message which contains IMSI (international mobile subscriber identity) information or TMSI (temporary mobile subscriber identity) information. Secret key K_i is determined from the IMSI or TMSI in the network according to a given function or by means of a table. The same key is also stored in smart card *SIM* in an inaccessible memory space. The secret key is required for later verification of the authentication process.

The network then initiates the authentication process by calculating random number *RAND* and transferring it via the air interface to smart card *SIM*.

Authentication parameter *SRES* is thereupon formed in the smart card by means of an authentication algorithm from secret key K_i and random number *RAND*, said parameter being in turn transferred via the air interface to the network. According to the invention, at least two random numbers $RAND_1$ and $RAND_2$ are derived from random number *RAND*. Random numbers $RAND_1$ and $RAND_2$ can be obtained by division or a selection from random number *RAND* or by a calculation algorithm.

Authentication is effected with a two-step algorithm in the example according to Fig. 1. First, as indicated in Fig. 1, first part $RAND_1$ of the random number is encrypted with first part K_1 of key K_i likewise split into two parts. The result of said first step is subsequently encrypted in a second step with second part K_2 of the key. For calculation with the authentication algorithm one can of course also use second part $RAND_2$ of the random number first and change the order of using first and second key parts K_1 and K_2.

Authentication parameter *SRES'* is meanwhile likewise formed in the network in the same way as in the card by means of the authentication algorithm and random number *RAND* ($RAND_1$, $RAND_2$) and secret key *Ki* (K_1, K_2). Parameter *SRES'* is then compared in the network with authentication parameter *SRES* obtained from the card. If authentication parameters *SRES'* and *SRES* match, the authentication process is completed successfully. If the authentication parameters do not match, the subscriber's card is regarded as unauthenticated. It should be noted here that one can also form *SRES* or *SRES'* using only parts of the result obtained by the encryption.

In the same way as the authentication parameters are generated, key *Kc* for channel coding for data and speech transmission is generated in the card and the network. One preferably uses as the input parameter the part of random number *RAND* not used in authentication.

Figure 2 shows an advantageous example by which calculation with the authentication algorithm and/or channel coding is executed by a triple DES algorithm. According to this algorithm, part $RAND_1$ or $RAND_2$ of the random number is first encrypted with first key part K_1. In the next step decryption is effected with K_2. The result is then encrypted with K_1 again or, if the random number/key is split into

a plurality of parts, with a third part of the key. The channel coding is formed in the same way. The corresponding algorithms are used in the network in each case.

Without restricting universality, the description of the examples according to Figs. 1 and 2 assumed a two- or three-step, symmetrical encryption algorithm. The inventive idea, which consists of splitting the random number and secret key, can of course also be executed with other, common encryption or calculation algorithms. By way of example, mention is made of not only the DES algorithms (A3; A8) but also IDEA. The stated algorithms can also be executed in one step, whereby different parts of the key and/or random number are preferably generated for authentication and generation of channel coding key *Kc*.

Figures 3*a* to *e* give examples of ways of splitting secret key K_i or random number *RAND*.

Figure 3*a* shows key K_i or random number *RAND* with a length of 128 bits.

Figure 3*b* shows a split into two equal parts K_1 and K_2 ($RAND_1$, $RAND_2$), the split being made in the middle. Part 1 contains bit 1 to bit 64, part 2 contains bit 65 to bit 128. Figure 3*c* shows an overlapping split, and Figure 3*d* shows a split by which the odd bits are assigned to part 1 and the even bits to part 2. Figure 3*e* finally shows a split by which the sum of the bit positions of parts 1 and 2 is smaller than the bit positions of the initial key or random number.